Commonwealth Office
of
Technology
Monthly Cyber Security Tips

What You need to Know About Botnets!

From the Desk of the Chief Information Security Officer

What is a bot? What is a botnet?

A **bot,** short for *robot,* is an automated software program that can execute certain commands. A **botnet,** short for *ro**bot net**work,* is an aggregation of compromised computers that are connected to a central "controller." The compromised computers are often referred to as "zombies."

Should I be concerned?

Yes-- Botnets are a significant problem on the Internet. They are a growing source for staging denial of service attacks, stealing personal information for identity theft, sending out email-based phishing attacks and spam. The compromised hosts or "zombies" are often home computers but business, government and education organizations are not immune. The sophisticated malicious code used by botnets make it difficult to detect by an untrained individual.

How does a bot infection happen?

Bot infections follow the same path as the typical Internet worm or virus. You may open an attachment in an email, visit a malicious web site or download malicious software often associated with "free software", such as games, screensavers, any of which may result in malware being installed on your computer. Once infected, the bot software sends a notice to the "controller." The controller then downloads additional malicious software to the compromised host. The botnet controller then may have complete control of your computer.

Examples of malicious software commonly associated with botnets and the subsequent activity impact on your computer are:

- ✓ Keystroke logger programs that specialize in capturing all of your key strokes and are adept at capturing personal information including your user name and password, as well as credit card and other financial information.
- ✓ Programs that are used to distribute spam. The next email you receive regarding a hot stock tip or prescription drugs could be coming from your neighbor. These emails usually employ a"spoofed" or phony email address.
- ✓ Denial of service attack programs. The botnet controller can summon tens of thousand of zombies to overwhelm web sites, computers or entire networks. Even large companies such as Microsoft, Yahoo and the *New York Times* have had their web sites impacted by denial of service attacks.

How prevalent are botnets?

Consider the following:
- ✓ According to Postini, an electronic messaging provider which processes over two billion messages a day, over 80% of email is spam.
- ✓ It is estimated that over 65% of spam worldwide is sent by botnets.
- ✓ The FBI recently reported a botnet containing over one million zombies!

How can I tell if my computer is part of a botnet?

If you are infected with a worm or virus, your chances are today that you may also be part of a botnet.

Some of the symptoms of infection are: your computer and Internet connection are slower than usual; programs that use to run on your computer no longer are able to run; your hard drive is spinning (making a noise) and you are not using your computer; or any other strange behaviors or anomalous activity on a computer.

If you detect any of the above your computer may be an indication of an infection and should be investigated further to determine if there is an infection, and if so, the type and the scale of the infection.

What can I do to protect my computer?

Bots propagate by taking advantage of security vulnerabilities in software, poor security controls, as well as by using social engineering techniques to entice users to open an email attachment that infects your computer or to visit a web site that downloads malware.

The following recommendations will help prevent your computer from becoming part of a botnet:
- ✓ Never open an email attachment unless you know what it is--even if it's from someone you know and trust.
- ✓ Do not visit untrusted web sites.
- ✓ Do not download free software from untrusted sites.
- ✓ Do not use free file sharing programs. These are commonly used to distribute music files and often contain malware.
- ✓ Use a firewall to filter Internet traffic.
- ✓ Use anti-virus and anti-spyware software and keep it up to date.
- ✓ Keep you operating system and application software, especially your Internet browser, up-to-date.

For more monthly tips go to:

http://technology.ky.gov/security/CyberAwareness.htm

http://www.msisac.org/awareness/news/

Brought to you by:

http://www.msisac.com

http://technology.ky.gov